

~28 BITS OF ENTROPY

2<sup>28</sup> = 3 DAYS AT 1000 GUESSES/SEC

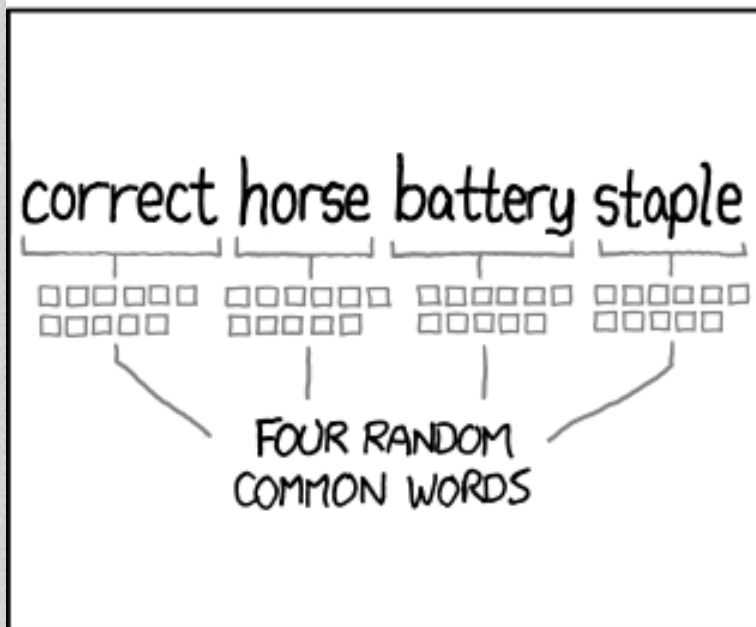
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: HARD



~44 BITS OF ENTROPY

2<sup>44</sup> = 550 YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS: HARD

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

# Passwords

*Diceware* hardware random number generator using dice

$$H = \log_2 N^L = L \log_2 N = L \frac{\log N}{\log 2}$$

<http://world.std.com/~reinhold/diceware.html>

Lets make a password!

*Keepass* <http://keepass.info/> Password manager

# Main Wallets

## Desktop wallets

Desktop wallets are installed on your computer. They give you complete control over your wallet. You are responsible for protecting your money and doing backups.



Bitcoin-Qt



MultiBit



Armory



Electrum

## Mobile wallets

Mobile wallets allow you to bring Bitcoin with you in your pocket. You can exchange bitcoins easily and pay in physical stores by scanning a QR code or using NFC "tap to pay".



Bitcoin  
Wallet



Mycelium  
Wallet



Blockchain  
.info

## Web wallets

Web wallets allow you to use Bitcoin on any browser or mobile and often offer additional services. However, you must choose your web wallet with care as they host your bitcoins.



Blockchain  
.info



Coinbase



Coinkite

# Wallet Grid

Wallet	Type	Width	Keys	Difficulty
Bitcoin QT	Desktop	Thick	Local	Medium/Advanced
Multibit	Desktop	Thin	Local	Easy
Armory	Desktop	Thick	Local	Advanced
Electrum	Desktop	Thin	Local	Easy
Bitcoin - Android	Android	Thin	Local	Easy
Mycelium	Android	Thin	Local	Easy
Blockchain	Android/Ipnone/Online	Thin	Non Local	Easy
Coinbase	Online	Thin	Non Local	Easy
Coinkite	Online	Thin	Non Local	?

# Hardware, Offline, Paper & Brain Wallets

Type	Storage	Example	Comments
Hardware	Keys offline on hardware device	Trezor	Expensive currently
Offline	Wallet file on offline computer	Electrum	Free
Paper	Wallet Seed written on paper	Electrum	Free
Brain Wallet	Memorise Seed	Electrum	Free

Key point here is to learn about these in your spare time. Do not experiment with any coins to begin with as mistakes happen. When you are comfortable you know what you are doing then proceed

Have a backup strategy! Eg say you have your coins on an offline computer and then it stops working! Where is your backup? Not a smart move and you will lose your coins. BE CONFIDENT BEFORE YOU STORE COINS USING ABOVE STRATEGIES

Next Electrum offline transaction

# Offline Transaction Demo

The screenshot shows the Electrum 1.9.4 wallet interface. The window title is "Electrum 1.9.4 - C:/Users/ronan/AppData/Roaming/Electrum/wallets/new [watching only]". The menu bar includes "File", "Wallet", "Tools", and "Help". Below the menu bar are tabs for "History", "Send", "Receive", "Contacts", and "Console". The main area displays a table of transaction history with the following data:

Date	Description	Amount	Balance
2014-01-27 21:50	14DFGkuedGnwQ82j9yetAJtS3QRpQAa7ip	+0.00150684	0.00150684

At the bottom left, the balance is displayed as "Balance: 0.00150684 BTC". At the bottom right, there are icons for a window, a settings gear, and a green status indicator.



# Other

BIPS :

[https://en.bitcoin.it/wiki/Bitcoin\\_Improvement\\_Proposals](https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals)

Cryptography : Branch of mathematics concerned with secure communication. Certain cryptographic functions and signatures assemble to secure the Bitcoin network

# Where to buy Bitcoin?

<b>Name</b>	<b>Type</b>	<b>Country</b>	<b>Comment</b>
Bitstamp	Online Exchange	Slovenia	Great Service
MtGox	Online Exchange	Japan	Liquid but slow withdrawals
BTC-e	Online exchange	Bulgaria	High Banking fees
Localbitcoins	P2P exchange	Global	Variable
Eircoin	Instant Bitcoin	Ireland	Instant

\*Exchanges are venues for matching buyers and sellers. You must deposit a balance with a provider to interact



# Bitcoin Trading

- Buying and then selling at a profit is fun ☐ The reverse is not. Bitcoin trading is high risk and not advised but lets look at an example

Example :

Day1: Buy 1 Bitcoin @ 90 USD

Day2: Sell 1 Bitcoin @ 100 USD

You now have 100USD in cash = 90 original +10 profit

If you trade a lot consider a LIFO or FIFO approach to keep track of profits

# Keeping Current, Getting Involved & Discussion

- <http://bitcoincharts.com/> : charts & tools
- <http://blockchain.info/> : charts & tools
- <http://www.coindesk.com/> : news
- <http://www.coinion.com/> : spoof news
- <https://bitcointalk.org/> : user forum
- <http://www.reddit.com/r/Bitcoin/> : reddit bitcoin

# Bitcoin Development

- <http://bitcoin.org/en/development>

You can get involved, contribute, write your own BIP, develop lesser used parts of Bitcoin, start your own business, accept Bitcoin as payment in daily life and/or evangelise